SMU | Dedman School of Law

SMU Law Review

Volume 70 | Issue 2 Article 10

2017

When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones

Efren Lemus

Southern Methodist University, elemus@mail.smu.edu

When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones

*Efren Lemus**

TABLE OF CONTENTS

* J.D. candidate, SMU Dedman School of Law, 2018; B.A. Psychology, Georgetown University, 2015. I dedicate this comment to my parents for their unwavering support and constant encouragement and my two brothers for being my greatest friends.

"[I]n the application of a Constitution, our contemplation cannot be only of what has been, but of what may be."[1]

I. INTRODUCTION

A. THE FACTS

IN May of 2016, controversy arose out of Los Angeles, California, after federal authorities obtained a search warrant "allowing the government to force people present when the warrant [was] executed to press their fingers and thumbs on the fingerprint sensors of any phones or computers found there to unlock them."[2] Although the warrant itself was not made public,[3] a memorandum[4] filed with the United States District Court for the Central District of California in support of the warrant application reveals the scope of the search these California authorities sought to carry out and their explanation as to why the warrant was constitutional.

1. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

2. Orin Kerr, *Can Warrants for Digital Evidence Also Require Fingerprints to Unlock Phones?*, WASH. POST (Oct. 19, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/19/can-warrants-for-digital-evidence-also-require-fingerprints-to-unlock-phones/?utm_term=.46b538fa904f [https://perma.cc/DEZ3-23WE].

3. Thomas Fox-Brewster, *Feds Walk into a Building, Demand Everyone's Fingerprints to Open Phones*, FORBES (Oct. 16, 2016), http://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/#2e3eec98d9d2 [https://perma.cc/5TMQ-WADB].

4. Notice of Filing Memorandum of Points and Authorities in Support of Search Warrant Application, Filed by United States Attorney for the Central District of California and Assistant United States Attorney (May 9, 2016), https://www.documentcloud.org/documents/3143273-Mass-Fingerprint-Case-Redacted-Copy-1.html [https://perma.cc/9SP8-EL2K] [hereinafter Memorandum].

> In the memorandum, U.S. attorneys detailed that they sought the warrant:
>
> > to use the fingerprints and thumbprints of *any person* who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant.[5]

The federal government's memorandum further requested authority to seize "passwords, encryption keys, and other access devices" to maintain access to the devices.[6] The memorandum stated that without the numerical or alpha-numerical passcodes to access the cellphones located within the subject premises, the government otherwise would not be able to obtain the contents of the devices if not authorized to use fingerprints and thumbprints to unlock them.[7]

The U.S. Attorney's Office for the Central District of California advanced various legal arguments in support of its search warrant. Specifically, the federal government argued that such a warrant would not violate the Fourth or Fifth Amendments of the Constitution.[8] For the sake of brevity and clarity, this Comment's focus will be solely on the government's Fifth Amendment conclusion.[9] Specifically, the Comment will focus on whether it is a violation of the Fifth Amendment right against self-incrimination for the government to compel individuals to press their fingerprint on their smartphone to unlock it and make its contents accessible.

1. The Government's Fifth Amendment Argument

The U.S. attorneys argued that "[c]ompelling a person to provide his or her fingerprint does not implicate, let alone violate, the Fifth Amendment."[10] Referencing the Supreme Court case of *Schmerber v. California*, the federal government stated that the Fifth Amendment does not protect individuals from compulsory fingerprinting because the Fifth Amendment does not concern itself with fingerprinting, but rather with protecting accused individuals from producing "testimonial or communicative evidence" against themselves.[11] Moreover, the government's memorandum stated that *Schmerber* clarifies that the prohibition of accused individuals providing testimonial or communicative evidence against themselves "[did] not apply to the use of a person's 'body as evidence

5. *Id.* at 1–2 (emphasis added).
6. *Id.* at 4 (quoting the warrant).
7. *Id.* at 3.
8. *Id.*
9. *See id.* at 5–7. Unlike the Fifth Amendment issue—or non-issue according to the federal government—the government acknowledged the existence of Fourth Amendment concerns but nonetheless maintained that the search warrant did not violate the Fourth Amendment. *Id.* at 5.
10. Memorandum, *supra* note 4, at 3.
11. *Id.* (quoting 384 U.S. 757, 761 (1966)).

when it may be material.'"[12] Thus, federal authorities in this case interpreted Fifth Amendment precedent to mean that government compulsion of "identifiable physical characteristics" does not violate the right against self-incrimination provided in the Constitution.[13]

Furthermore, the government cited Ninth Circuit precedent to argue that "fingerprint evidence from a defendant or a suspect are not prohibited by the Fifth Amendment right against self-incrimination because such evidence is not testimonial in nature."[14] While federal authorities conceded that "the government does not know ahead of time the identity of every digital device or fingerprint . . . that it will find in the search," it asserted that it "demonstrated probable cause that evidence may exist at the search location" and, therefore, required "access to those devices" and the ability to "maintain that access to search them."[15] Therefore, the U.S. Attorney's Office for the Central District of California contended that because a fingerprint is an identifiable physical characteristic and not testimonial or communicative evidence, then the privilege against self-incrimination did not apply in this situation.[16]

2. Criticism of Such Practices

The search warrant in this case raises potential constitutional issues on Fifth Amendment grounds, particularly with respect to the right against self-incrimination.[17] Experts have warned of the lack of legal protections that exist in the area of fingerprint technology to prevent infringement of basic constitutional rights.[18] Despite federal authorities in this case asserting that their actions did not violate the Fifth Amendment guarantee against self-incrimination, others have voiced their "shock" at the situation and view it as an "unprecedented attempt to bypass the security of . . . smartphone[s] that use[ ] fingerprints to unlock."[19] Others question whether authorities are simply seeking such warrants to get more information after executing the warrants, rather than basing their warrant requests on already existing facts that raise reasonable suspicion.[20]

These attempts have been denounced as "inventive" ways for law enforcement officials to try to legally penetrate through the security of

12. *Id.* (quoting *Schmerber*, 384 U.S. at 763).

13. *Id.* (quoting United States v. Dionisio, 410 U.S. 1, 5–6 (1973)).

14. *Id.* at 4 (quoting Commonwealth of N. Marian Islands v. Bowie, 243 F. 3d 1109, 1120 n.5 (9th Cir. 2001); citing Virginia v. Baust, 89 Va. Cir. 267 (Oct. 28, 2014) ("holding that defendant could be compelled to provide his fingerprint in order to unlock phone")).

15. Memorandum, *supra* note 4, at 4.

16. *See id.* at 3–4.

17. *See* Kerr, *supra* note 2.

18. Lorenzo Franceschi-Bicchierai, *Cops Can Make You Unlock Your Smartphone with Fingerprint, Says Judge*, MASHABLE (Oct. 30, 2014), http://mashable.com/2014/10/30/cops-can-force-you-to-unlock-phone-with-fingerprint-ruling/ [https://perma.cc/39NN-LJGX].

19. Fox-Brewster, *supra* note 3.

20. *Id.*

smartphones, as new legal and technical barriers hinder their efforts.[21] Criminal defense attorney Marina Medvin stated that the government is "seeking to have the ability to convince people to comply by providing their fingerprints to law enforcement under the color of law – because of the fact that they already have a warrant."[22] Andrew Crocker, a staff attorney at the Electronic Frontier Foundation (EFF), opined that using warrants to compel the production of fingerprints, rather than potentially self-incriminating passwords, to unlock phones was a "'clever end-run' around constitutional rights."[23]

Crocker also seriously questioned the wide-reaching scope of these warrants.[24] He questioned whether the Fourth Amendment, which protects against unreasonable search and seizure, "allows such an open-ended extension of the search warrant."[25] Crocker noted that despite search warrants needing to be "narrow and clear in scope," the warrant in this case unnecessarily extended to every phone in the property and all of the private information contained in them.[26] Another EFF attorney, Jennifer Lynch, also scrutinized the specificity and particularity of these warrants.[27] Lynch argued that "[t]he government needs to say specifically what information they expect to find on the phone, how that [information] relates to criminal activity and . . . to access only the information that is relevant to the investigation."[28] Lynch added that the warrant's scope must be limited and describe the place and people to be searched with particularity.[29]

B. Overview of Comment

The implications of the government's request and the growing prevalence of fingerprint and other biometric data implemented in personal devices[30] warrant a discussion on the constitutionality of such practices as they relate to the Fifth Amendment privilege against self-incrimination. Such a discussion is not only timely, but also urgent, if our legal system is to develop in unison with technological and societal developments. Novelty is also a factor that calls for this discussion because, as it has been

21. *Id.* Technical difficulties law enforcement officials encounter involve, for example, the disabling of fingerprint authentication in iPhones (TouchID) after 48 hours of not using the feature or rebooting the cellphone. *See About Touch ID Security on iPhone and iPad*, Apple: Support (Nov. 3, 2015), https://support.apple.com/en-us/HT204587 [https://perma.cc/M99M-6BB9] [hereinafter *Touch ID*].

22. Fox-Brewster, *supra* note 3.

23. Karen Turner, *Feds Use Search Warrants to Get into Fingerprint-Locked Phones*, Wash. Post (Oct. 18, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/18/feds-use-search-warrants-to-get-into-fingerprint-locked-phones/?utm_term=.C87ea405c186 [https://perma.cc/WY9Y-DESC].

24. *Id.*

25. *Id.*

26. *Id.*

27. Fox-Brewster, *supra* note 3.

28. *Id.*

29. *Id.*

30. *See* discussion *infra* Part II.

correctly pointed out, "[t]his scenario presents the courts with an issue of first impression, because in the past, a fingerprint was merely used as a method of identification"[31] and not as a key that grants access to a person's most sensitive information.

Critically, the discussion should focus on the *principles* underwriting the Fifth Amendment right against self-incrimination. When new developments—whether technological, social, or political in nature—significantly challenge the perceptions and notions Americans have of their basic Constitutional rights, it becomes imperative to take a principled look at these constitutionally-protected guarantees to ensure that these new developments are adapted to conform to the Constitutional framework, rather than vice-versa. To do otherwise would be to compromise the foundations of our legal system, and by consequence, our legal rights, to the caprices of the world's happenings.

Even though constitutional analysis of cell phone searches has mostly focused around the Fourth Amendment, "the Fifth Amendment is emerging in importance as access to . . . cellular phone[s] advances."[32] Using current precedent and taking into account the principle of "privacy" that serves as a justification for the privilege against self-incrimination, this Comment will examine the Fifth Amendment theories set forth by federal authorities in the Los Angeles case[33] and other arguments that have been advanced to endorse this type of activity. For purposes of this Comment, it will be assumed that, like the executed warrant described in the introduction, the government compels undescribed individuals inside of subject premises to unlock their cell phones using their fingerprints and finds incriminating information inside of those devices. Therefore, the issue this Comment seeks to elucidate is whether incriminating evidence obtained by an individual's act of unlocking his phone using his fingerprint under government compulsion violates that individual's right against self-incrimination. Finding an appropriate answer to this question turns on whether the act of pressing a fingerprint onto a phone to unlock it and make its contents accessible qualifies as "testimonial" activity.[34]

Part II of this Comment will provide information on the ubiquitous character of smartphone and other digital technologies.[35] Part II will also detail how smartphone devices increasingly contain more private information of individuals.[36] Thereafter, Part II will discuss how fingerprint and other biometric data features have been integrated as encryption mechanisms into these devices to strengthen their security.[37] A discussion will also be provided on how federal and other law enforcement authori-

31. Kara Goldman, Note, *Biometric Passwords and the Privilege Against Self-Incrimination*, 33 CARDOZO ARTS & ENT. L.J. 211, 215 (2015).
32. Kristen Vogl, *Isearch into the Iphone*, 20 J. TECH. L. & POL'Y 179, 180 (2015).
33. *See* Fox-Brewster, *supra* note 3; Kerr, *supra* note 2.
34. *See generally* Holt v. United States, 218 U.S. 245 (1910).
35. *See infra* Section II.A.
36. *See infra* Section II.A.
37. *See infra* Section II.B.

ties use data in mobile devices in their investigations.[38]

Part III will analyze whether compelling individuals to depress their fingerprints on smartphone devices to unlock them amounts to a violation of the constitutional right against self-incrimination.[39] To place the analysis in context, Part III will give an overview of Supreme Court precedent regarding the Fifth Amendment right against self-incrimination,[40] and it will address how lower courts have used this precedent in cases involving both encryption in technological devices and the privilege against self-incrimination.[41] Part III will also discuss the foregone conclusion doctrine.[42]

Part IV of this Comment will analyze whether these cases, and more importantly, warrants issued to access smartphones using fingerprints, implicate the Fifth Amendment right against self-incrimination.[43] Although it previously has been suggested that government compulsion to unlock a cell phone using fingerprints "falls well within the scope of rights afforded by the Fifth Amendment,"[44] this Comment suggests that it does not under the current state of the law. However, courts should devise new standards for these situations based on principles of privacy that undergird the right against self-incrimination. Therefore, this Comment advances the proposition that, even though the warrant issued in the California case is not unconstitutional under current jurisprudence concerning the Fifth Amendment right against self-incrimination, courts should devise a new standard based on the principle of privacy to address these situations.

II. BACKGROUND ON MOBILE DEVICES, BIOMETRIC INFORMATION, AND THEIR ROLE IN CRIMINAL INVESTGATIONS

A. The Ubiquity of Mobile Devices and Growth of Fingerprint Authentication

One of the safest assumptions a person could make in today's America is that any random individual walking down the street is likely carrying a smartphone. Smartphones have become virtually synonymous with necessity and may be reasonably characterized as "extensions of ourselves."[45] Commenting on the ubiquity of these devices, Chief Justice Roberts has previously remarked that smartphones "are now such a pervasive and in-

38. *See infra* Section II.C.
39. *See generally infra* Part III.
40. *See infra* Section III.A.
41. *See infra* Section III.C.
42. *See infra* Section III.B.
43. *See generally infra* Part IV.
44. Goldman, *supra* note 31, at 228.
45. *See* Michael Lynch, *Leave My iPhone Alone: Why Our Smartphones Are Extensions of Ourselves*, The Guardian (Feb. 19, 2016), https://www.theguardian.com/technology/2016/feb/19/iphone-apple-privacy-smartphones-extension-of-ourselves [https://perma.cc/W8YW-KK59].

sistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[46]

According to the Pew Research Center, 95% of Americans own a cell phone of some kind, while 77% own cell phones considered to be "smartphone" devices.[47] A 2015 study conducted by the professional services firm Deloitte "found that Americans collectively check their smartphones upwards of 8 billion times per day," meaning that across age groups, the average American checks his or her phone forty-six times in one day.[48]

Americans not only use their cell phones regularly, but the activities they use them for are often private in nature. The Pew Research Center found that 67% of Americans use their cell phones to share intimate information about their personal lives like "pictures, videos, or commentary about events happening in their community, with 35% doing so frequently."[49] Furthermore, a study from 2012 revealed that a majority of Americans not only use their cell phones to share these intimate details of their personal lives, but also that roughly half of America's cell phone users create back-up files of this data on their phones,[50] signaling how much value they place on this information.

Other data gathered by the Pew Research Center showed that most Americans use their smartphones for very private reasons such as looking up specifics on their health conditions and engaging in online banking, while a substantial portion of the smartphone-using population use their devices for other personal reasons like job searching or submitting job applications.[51] In fact, as of early 2013, 78% of mobile technology users believed the information contained in their mobile devices to be as private as that stored in traditional computers.[52] As the Supreme Court has astutely recognized, to call modern mobile devices merely cell phones is "misleading" because "[t]hey could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums,

---

46. Riley v. California, 134 S. Ct. 2473, 2484 (2014).

47. *Mobile Fact Sheet*, PEW RESEARCH CTR. (Jan 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/FUH8-F434].

48. Lisa Eadicicco, *Americans Check Their Phones 8 Billion Times a Day*, TIME (Dec. 15, 2015), http://time.com/4147614/smartphone-usage-us-2015/ [https://perma.cc/M6TF-UZ89].

49. Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/ [https://perma.cc/S64H-Z9WD].

50. Jan L. Boyles, Aaron Smith, & Mary Madden, *Main Findings: Apps and Privacy: More Than Half of App Users Have Uninstalled or Decided to Not Install an App Due to Concerns About Their Personal Information*, PEW RESEARCH CTR. (Sep. 15, 2012), http://www.pewinternet.org/2012/09/05/main-findings-7/ [https://perma.cc/6CTK-W87W].

51. *See* Smith, *supra* note 49.

52. John B. Kennedy & Annie C. Bai, *Reining in Mobile App Privacy Practices*, LAW 360 (JAN. 25, 2017, 12:23 PM), HTTP://WWW.LAW360.COM/ARTICLES/407974/REINING-IN-MOBILE-APP-PRIVACY-PRACTICES [HTTPS://PERMA.CC/CSH6-U8FL] (CITING JENNIFER M. URBAN, CHRIS JAY HOOFNAGLE & SU LI, *Mobile Phones and Privacy* (U.C. Berkeley Public Law Research Paper No. 2103405, 2012), https://iapp.org/media/pdf/knowledge_center/Mobile_phones_and_privacy.pdf [https://perma.cc/DS8V-H9YB]).

televisions, maps, or newspapers."[53]

Moreover, Americans are not oblivious to the inherent privacy dangers smartphone devices possess. Significantly, "54% of app users have decided to not install a cell phone app once they discovered how much personal information they would need to share in order to use it."[54] Given the swelling dependency on mobile devices for everyday use,[55] it is reasonable to conclude that all of these data figures have meaningfully increased since these studies were conducted.

Thus, it is evident that Americans widely use smartphone devices and that they associate a high level of privacy with them. People use smartphones for a variety of personal reasons, including communicating with family and friends, online banking, and storing photos.[56] The private nature of the activities performed on mobile devices makes encryption of these devices not only convenient, but necessary. Thus, many technology companies have developed devices that may be easily encrypted and often make encryption mechanisms default features on their devices.[57]

B. Fingerprint Sensors as Unlocking Mechanisms in Cellphones

The ubiquity of these new technologies and the personal and intimate activities they are used for invariably raise concerns over how individual privacy may be affected.[58] At the center of these concerns is whether and how both industry and the legal system will ensure that our fundamental rights are not infringed in this new era of digital privacy. On a technical level, technology companies have responded to these privacy concerns by implementing encryption into their devices.[59]

Fundamentally, encryption is a method that makes data inaccessible by converting understandable information into an incomprehensible amalgam of numbers and letters.[60] The purpose of encryption is to safeguard information and "make[ ] it undecipherable to third parties" by using a password, or any other method of verification or authentication, to block access to that information.[61] Cryptography, the study of encryption, examines "how parties safeguard important information on personal de-

53. Riley v. California, 134 S. Ct. 2473, 2489 (2014).
54. Jan L. Boyles, Aaron Smith, & Mary Madden, *supra* note 50.
55. *See* Smith, *supra* note 49.
56. *See id.*
57. *See iOS Security: iOS 10*, Apple (Mar. 2017), https://www.apple.com/business/docs/iOS_Security_Guide.pdf [https://perma.cc/3KMP-PPXU] ("By setting up a device passcode, the user automatically enables Data Protection.").
58. *See* Matthew Whitten, *Attacking Analogies: The Need for Independent Standards for Mobile Privacy*, 19 UCLA J.L. & Tech. 1, 1 (2015).
59. *See infra* note 71 and accompanying text.
60. *See A Brief History of Cryptography*, Cypher Res. Laboratories, http://www.cypher.com.au/crypto_history.htm [https://perma.cc/Z25L-AFJ3] (last visited Jan. 6, 2017).
61. Michael Wachtel, *Give Me Your Password Because Congress Can Say So: An Analysis of Fifth Amendment Protection Afforded Individuals Regarding Compelled Production of Encrypted Data and Possible Solutions to the Problem of Getting Data from Someone's Mind*, 14 U. Pitt. J. Tech. L. & Pol'y 44, 47 (2013).

vices, such as computers, by using passwords as a form of encryption."[62] Whenever anyone—"including the government acting in [its] . . . investigatory capacity"—attempts to decrypt an encrypted device, they seek to access the "plaintext," or the underlying data that is protected through encryption.[63]

An "encryption key" is required to fully decrypt an encrypted device.[64] Encryption keys are a series of number sequences "stored in the encryption software's memory" that are lengthy and complex.[65] Passwords and other verification and authentication tools, when entered into a device, trigger the encryption key and grant access to the data contained in the device.[66] Thus, "[w]hen the government 'seeks to compel [individuals] to'" decrypt their devices, they look for production of the verification or authentication tool (be it a password or, for our purposes, a fingerprint) used to trigger the encryption key, "rather than the intricate encryption key" itself.[67]

The advent of encryption has revolutionized how we perceive our mobile devices. Nowadays, smartphone devices "are in many respects akin to a safe" because people often use them to protect information that they wish to keep private, which they readily can accomplish with encryption.[68] One form of encryption uses biometric data instead of numerical or alphabetical passwords as an authentication source to protect information.[69] Fingerprint authentication, or the matching of a unique fingerprint to a device to unlock it, is an example of such biometric encryption used to protect sensitive information in electronic devices.[70] "Apple Inc., Motorola, HTC, and Samsung"—among other prominent cellphone manufacturers—have equipped their newest devices with fingerprint sensors that may serve as "unlocking" devices.[71] Using these sensors, users may set up a security feature on their phones which allows them to unlock their phones by simply pressing their unique finger or thumbprints on the sensor.[72] If the finger or thumbprint pressed onto the sensor matches the one that was used to initially set up this feature, the phone will unlock.[73] The integration of biometric data as a source of authentication to secure devices reduces the mental taxation of users by avoiding the necessity of

62. *Id.*
63. *Id.*
64. *Id.* at 48.
65. *Id.*
66. *Id.*
67. Wachtel, *supra* note 61, at 48 (quoting Brendan M. Palfreyman, *Lessons from the British and American Approaches to Compelled Decryption*, 75 BROOK. L. REV. 345, 350-51 (2009)).
68. *Id.* at 46.
69. Colin Soutar et al., *Biometric Encryption*, *in* ICSA GUIDE TO CRYPTOGRAPHY 1–2 (Randall K. Nichols ed., 1999), http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf [https://perma.cc/EMH7-UY8X].
70. *See id.* at 4–5.
71. Memorandum, *supra* note 4, at 1.
72. *Id.*
73. *Id.*

memorizing number or letter sequences.[74]

In 2013, when Apple Inc. released its highly-anticipated iPhone 5s, "the most forward-thinking smartphone in the world," one of the phone's most appealing features was its implementation of the Touch ID finger sensor.[75] Apple described the Touch ID feature as "an innovative way to simply and securely unlock your iPhone with just the touch of a finger."[76] Praising this innovative biometric feature, Apple says of their Touch ID feature: "Your fingerprint is one of the best passcodes in the world. It's always with you, and no two are exactly alike."[77]

The integration of these biometric features in smartphones reflects an overarching trend in the growth of fingerprint recognition and other biometric data used in mobile technologies. According to the research group Research and Markets, the total market value of the "fingerprint recognition and mobile biometrics market" is projected to grow at an annual rate of 215.49% between the years 2014 and 2019.[78] Biometric authentication is not only on a course of proliferation, but it is also headed in complex directions as smartphone manufacturers look beyond fingerprint readers and into retina scanners to strengthen the security of their devices.[79]

The trend toward biometric authentication meaningfully departs from prior methods used to secure mobile devices such as numerical passwords. Although these technological features in smartphones are becoming pervasive, concerns about the desirability of these features have nonetheless been raised. This is especially true with regard to hacking; the creation of backdoors to send stored fingerprint information to governments or third parties; and, importantly, the possible loophole it creates for law enforcement officials to bypass certain constitutional rights of the accused.[80] It is incumbent upon the legal system to systemically address

---

74. Marco Tabini, *Open Sesame: How iOS 8 Will Unlock Touch ID's Power,* MACWORLD (July 22, 2014, 5:00 AM), http://www.macworld.com/article/2455474/open-sesame-how-ios-8-will-unlock-touch-ids-power.html [https://perma.cc/V2PF-5KQS].

75. *Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World*, APPLE: PRESS RELEASES (Sept. 10, 2013), http://www.apple.com/pr/library/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World.html [https://perma.cc/KY3G-QQN6].

76. *Id.* ("Touch ID uses a laser cut sapphire crystal, together with the capacitive touch sensor, to take a high-resolution image of your fingerprint . . . All fingerprint information is encrypted and stored securely in the Secure Enclave inside the A7 chip on the iPhone 5s; it's never stored on Apple servers or backed up to iCloud®.").

77. *Touch ID*, *supra* note 21.

78. *Global Fingerprint Mobile Biometrics Market - Research Report 2015-2019*, RESEARCH AND MARKETS (Oct. 2015), http://www.researchandmarkets.com/research/rxxnls/global [https://perma.cc/4NJ6-CP8G].

79. Lance Whitney, *Galaxy S7 May Sport Retina Scanner with Pressure Sensitive Display*, CNET (Dec. 14, 2015, 7:28 AM), http://www.cnet.com/news/samsung-galaxy-s7-might-sport-pressure-sensitive-display/ [https://perma.cc/GT3G-CWMF].

80. *See* Rafe Needleman, *The 2 Big Problems with Fingerprint Security*, YAHOO TECH (Jan. 28, 2015), https://www.yahoo.com/tech/the-2-big-problems-with-fingerprint-security-109371608679.html [https://perma.cc/KQK7-JGTQ]; Joseph Steinberg, *Why You Should Not Use the New Smartphone Fingerprint Readers*, FORBES (Mar. 5, 2015), http://www.forbes.com/sites/josephsteinberg/2015/03/05/why-you-should-not-use-the-new-smartphone-fingerprint-readers/#22d002521aa8 (Perma link unavailable); Alastair Stevenson, *Hackers*

the legal challenges such a technological shift brings with respect to how the government can access the information contained in the smartphone devices of its citizens.

C. The Growing Importance of Cellphone Data in Law Enforcement Activity

Considering the wealth of personal information stored in mobile devices, the government naturally seeks warrants granting them permission to access the devices of individuals they suspect of committing, or being involved in, crimes. For instance, "[i]n 2012, federal and local law enforcement agencies made more than 1.1 million requests for the personal cellphone data of Americans for a variety of investigative reasons."[81] However, because most smartphone devices are encrypted, law enforcement's only way of making the information in mobile devices accessible and readable is by having the user of the device provide his passcode or other form of authentication.[82] Consumer control over encryption poses an issue for law enforcement because it leaves the person being investigated as the only party capable of decrypting his or her device and making the information readily available.[83] Because of this, law enforcement officials have advocated for less secure encryption methods to facilitate their activities.[84]

Amidst this growing governmental interest in accessing the information stored in its citizens' mobile devices, it is important to be aware of the methods they employ to accomplish this and, more importantly, to consider whether those methods respect basic constitutional rights. As previously explained, this Comment will analyze if an individual's Fifth Amendment right against self-incrimination is violated when the government compels him to press his fingerprints on his phone to unlock it and make its contents accessible. Although under current Supreme Court jurisprudence lower courts are likely to hold that this is not a violation of

---

Can Remotely Steal Your Identity Using Android Fingerprint Scanners, Business Insider (Aug. 7, 2015, 7:23 AM), http://www.businessinsider.com/android-phones-fingerprint-scanners-have-serious-security-vulnerabilities-2015-8 [https://perma.cc/3KQD-J8YG].

81. Tom Jackman, *Experts Say Law Enforcement's Use of Cellphone Records Can Be Inaccurate*, Wash. Post (June 27, 2014), https://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html?utm_term=.dac740becb0a [https://perma.cc/MBA7-EX39] (data compiled from a privacy-related survey undertaken by Sen. Edward J. Markey of Massachusetts).

82. Matthew J. Weber, Note, *Warning—Weak Password: The Courts' Indecipherable Approach to Encryption and the Fifth Amendment*, 2016 U. Ill. J.L. Tech. & Pol'y 455, 460 (2016).

83. *Id.* at 456 (citing *Legal Process Guidelines: U.S. Law Enforcement*, Apple (Sept. 29, 2015), http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/7H7J-GF3T]).

84. Manhattan Dist. Attorney's Office, Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety 13 (Nov. 2015), https://cyber.harvard.edu/pubrelease/dont-panic/DA_Report_Smartphone_Encryption_Public_Safety_11182015.pdf [https://perma.cc/4BQN-7WLX].

the right against self-incrimination,[85] courts should endeavor to fashion a new standard that places at its core the principle of privacy. Doing so will give greater protection to the private lives of citizens, which are increasingly contained in their smartphones.

III. CURRENT STATE OF THE RIGHT AGAINST SELF-INCRIMINATION

The Fifth Amendment guarantees the privilege to be free from self-incrimination, stating that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[86] This privilege is understood to most strongly reflect the American judicial system's preference for an "accusatorial, not inquisitorial" criminal procedure.[87] However, notwithstanding its significance to the criminal justice system, judges and commentators have struggled to identify the privilege's central policy objectives or how far it should extend.[88] Justice Harlan notably remarked: "The Constitution contains no formulae with which we can calculate the areas . . . to which the privilege should extend, and the Court has therefore been obliged to fashion for itself standards for the application of the privilege."[89] Generally, the Supreme Court has interpreted the self-incrimination clause as prohibiting the government from compelling an individual to testify against himself or from compelling an individual to offer testimonial evidence that would be self-incriminatory.[90] Thus, "for the privilege to apply, the communication the defendant is attempting to protect must be compelled, testimonial, and incriminating in nature."[91] If these three requirements are not met, then the privilege is not implicated. As is the case for the Constitution generally, the Fifth Amendment's language is subject to broad interpretation and has invited courts to expand its meaning far beyond its literal terms.[92] Particularly contentious has

85. *See infra* Section III.A.

86. U.S. CONST. amend. V.

87. Malloy v. Hogan, 378 U.S. 1, 7 (1964).

88. Robert B. McKay, *Self-Incrimination and the New Privacy*, 1967 SUP. CT. REV. 193, 193–94 (1967).

89. Spevack v. Klein, 385 U.S. 511, 522 (1967) (Harlan, J., dissenting); *see* Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 56 n.5 (1964) (quoting Harry Kalven, Jr., *Invoking the Fifth Amendment—Some Legal and Impractical Considerations*, 9 BULL. ATOMIC SCIENTISTS 181, 182 (1953)).

90. *See* United States v. Hubbell, 530 U.S. 27, 43 (2000); Fisher v. United States, 425 U.S. 391, 409 (1976).

91. Nicholas Soares, Note, *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, 49 AM. CRIM. L. REV. 2001, 2004 (2012) (citing Fisher v. United States, 425 U.S. 391, 408 (1976) ("stating that the >Fifth Amendment privilege against self-incrimination applies only when the accused is compelled to make a testimonial communication that is incriminating")); *see also* United States v. Authement, 607 F.2d 1129, 1131 (5th Cir. 1979).

92. Lisa Tarallo, Note, *The Fifth Amendment Privilege Against Self-Incrimination: The Time Has Come for the United States Supreme Court to End Its Silence on the Rationale Behind the Contemporary Application of the Privilege*, 27 NEW ENG. L. REV. 137, 137 (1992).

been judicial interpretation of what encompasses "testimonial" activity.[93]

A. Supreme Court and the Right Against Self-Incrimination

As early as 1886, the Supreme Court struggled to define what actions can be properly characterized as testimonial in nature.[94] In *Boyd v. United States*, the Court found that the privilege against self-incrimination applied when a court ordered a defendant to turn over documents that were intended to evince criminal conduct of the defendant.[95] The Court reasoned that the governmental order to produce the incriminating documents was a way of forcibly extracting testimony out of an individual in violation of his constitutional right to be free from self-incrimination under governmental compulsion.[96] In the *Boyd* Court's view, the "seizure of a man's . . . papers" is fundamentally tantamount to "compelling him to be a witness against himself."[97] Thus, in this instance, the Court regarded compelled documents as mere substitutes for the compelled testimony of an individual against himself.

Following *Boyd*, in *Holt v. United States*, the Court narrowed the privilege against self-incrimination by attempting to create a distinction between "physical" evidence and "communicative," or "testimonial," evidence.[98] In *Holt*, a defendant asserted his right against self-incrimination to suppress evidence that a specific incriminating shirt fit him after the government had compelled him to try it on.[99] Writing for the majority, Justice Holmes rejected the defendant's attempted use of the privilege calling it "an extravagant extension of the [Fifth] Amendment."[100] Holmes noted that the privilege is only intended to protect communicative evidence, which does not encompass the "body as evidence when it may be material."[101] Therefore, by drawing this distinction, the Court seemed to suggest that the right against self-incrimination applied only to evidence that could be communicated in some form or another and not to evidence that was merely physical.

In *Schmerber v. California*, the Supreme Court adopted the same reasoning used by Justice Holmes in *Holt*. The Court held that government compulsion of an individual to furnish a blood sample, although potentially incriminating, did not fall within the privilege because it is a non-communicative, non-testimonial act.[102] The *Schmerber* decision not only

93. *See id.* at 147–52; *see also* Jody C. Barillare, Comment, *As Its Next Witness, the State Calls . . . the Defendant: Brain Fingerprinting as "Testimonial" Under the Fifth Amendment*, 79 Temp. L. Rev. 971, 982 (2006).
94. *See* Boyd v. United States, 116 U.S. 616 (1886).
95. *Id.* at 633.
96. *Id.* at 630.
97. *Id.* at 633.
98. 218 U.S. 245, 252–53 (1910).
99. *Id.* at 252.
100. *Id.*
101. *Id.* at 252–53.
102. Schmerber v. California, 384 U.S. 757, 764 (1966). The U.S. Attorney's Office for the Central District of California heavily relied on this case to argue that the warrant com-

established the rule that compelled blood samples are not testimonial in nature, but its reasoning also clarified the physical versus communicative distinction Justice Holmes established in *Holt*.[103]

In explaining its holding, the *Schmerber* Court noted that although the government had compelled the defendant to unwillingly participate in the collection of evidence used to incriminate him by forcing him to furnish a blood sample,[104] providing a blood sample is not testimonial.[105] The Court explained that "the privilege is a bar against compelling 'communications' or 'testimony,' but . . . compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it."[106] The defendant's participation in the extraction of the blood sample was irrelevant because the results of the test did not depend on the defendant's efforts, but rather on an independent chemical analysis.[107]

However, the Court qualified that, sometimes, there will be "cases in which such a distinction [between physical and testimonial evidence] is not readily drawn."[108] Such a qualification impliedly recognizes that physical evidence at times may possess communicative attributes. Furthermore, the Court curiously noted that if its understanding of the privilege's scope fully comported with the principles the privilege helps protect—including "the inviolability of the human personality"[109]—then the Court likely would have concluded that the privilege was in fact violated in this case.[110]

A year after *Schmerber*, the Supreme Court further restricted the meaning of "testimonial" in *United States v. Wade*.[111] In *Wade*, the Supreme Court considered a situation where the government compelled a defendant to stand in a lineup and speak words that were uttered by a bank robber so that bank employees could identify the actual perpetrator.[112] The bank employees identified the defendant's voice as that of the bank robber in the lineup and at trial as the person who robbed the bank.[113] The defendant's counsel objected to the courtroom identification, claiming that compelling the defendant to stand in the lineup and utter the words of the bank robber "violated his Fifth Amendment [right] against self-incrimination."[114] The Court rejected this proposition,[115] observing that standing in the lineup and vocalizing a phrase was "compul-

---

pelling individuals to press their fingerprints on their smartphones to unlock them did not violate the right against self-incrimination. *See* Memorandum, *supra* note 4, at 3.

103. *See Schmerber*, 384 U.S. at 765; *see also supra* text accompanying note 98.
104. *Schmerber*, 384 U.S. at 761.
105. *Id.* at 765.
106. *Id.* at 764.
107. *Id.* at 765.
108. *Id.* at 764.
109. *Id.* at 762 (quoting Miranda v. Arizona, 384 U.S. 436, 460 (1966)).
110. *Schmerber*, 384 U.S. at 762.
111. 388 U.S. 218 (1967).
112. *Id.* at 220.
113. *Id.*
114. *Id.*
115. *Id.* at 221.

sion of the accused to exhibit his physical characteristics, not compulsion to disclose any knowledge he might have."[116] Thus, in the Court's view, compelling the accused to speak in this case was not testimonial because his speech was used "as an identifying physical characteristic, not to speak his guilt."[117]

In 1988, the Supreme Court sought to consolidate the holdings and rationales of Fifth Amendment self-incrimination cases to develop a clearer and more precise picture of what constitutes testimonial or communicative evidence covered under the privilege.[118] In *Doe v. United States*, the issue before the Court was whether the government could compel an individual to sign a consent form that would authorize financial institutions to release records of his bank accounts that could reveal evidence of financial fraud.[119] Upon examining the Court's precedent on the privilege, Justice Blackmun, writing for the majority, concluded that "to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself."[120] Using this rationale, the Court held that compelling a defendant to sign a consent form allowing the release of potentially incriminating financial documents would not implicate the privilege against self-incrimination because "neither the form, nor its execution, communicates any factual assertions, implicit[121] or explicit, or conveys any information to the [g]overnment."[122]

"[T]he [Fifth] Amendment does not protect against the self-disclosure of all incriminating evidence."[123] The Supreme Court in *United States v. Hubbell*[124] helped clarify which type of activity could rise to the level of incriminating testimonial evidence. In *Hubbell*, the Court held that a defendant's Fifth Amendment right against self-incrimination could be violated if the government compelled the defendant to produce documents that could *lead* to potentially incriminating evidence.[125] Additionally, the Court added that in producing documents "[i]t was unquestionably neces-

116. *Id.* at 222. Similar Court rulings and reasoning include United States v. Dionisio, 410 U.S. 1, 7 (1973) (holding that the government may compel a voice recording because it falls outside of the scope of the privilege since it is being compelled to identify physical properties of the voice and not to analyze the content of vocalizations); Gilbert v. California, 388 U.S. 263, 266–67 (1967) (holding that the government can compel a suspect to provide a handwriting sample because a handwriting sample is an identifying physical characteristic that stands outside the protection of the privilege, despite the fact that handwriting is typically used as a communicative device).

117. *Wade*, 388 U.S. at 222–23.

118. *See* Doe v. United States, 487 U.S. 201 (1988).

119. *Id.* at 202–03.

120. *Id.* at 208–10.

121. *See* Fisher v. United States, 425 U.S. 391, 410–11 (1976) (stating that the act of production may rise to the level of testimonial activity because it could communicate implicit statements of fact such as that the produced content exists, is in the control of the accused, and is authentic).

122. *Doe*, 487 U.S. at 215.

123. *See* Soares, *supra* note 91.

124. 530 U.S. 27 (2000).

125. *Id.* at 43.

sary for respondent to make extensive use of 'the *contents of his own mind*' in identifying the hundreds of documents responsive to the requests in the subpoena."[126] The majority opinion observed that the mental exertion implicated in assembling documents could constitute a testimonial act because "[t]he assembly of those documents [is] like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox."[127] Therefore, after *Hubbell*, the Court seemingly shifted its rationale in self-incrimination cases from the physical versus testimonial dichotomy to an analysis focused on whether the suspect used his mental faculties to help the government assemble its case.

B. A Brief Overview of the Foregone Conclusion Doctrine

It is necessary to mention an exception to the Fifth Amendment privilege against self-incrimination known as the foregone conclusion doctrine, albeit briefly, for the purposes of this Comment.[128] The foregone conclusion doctrine provides that a compelled act of production is not testimonial whenever the information conveyed is already known by the government, such that the individual "adds little or nothing to the sum total of the [g]overnment's information."[129] For the doctrine to apply, the government must show with reasonable particularity that when it compelled the individual to produce the information it wanted, it already knew the evidence sought existed, the evidence was in the possession of the accused, and the evidence was authentic.[130] If the government can establish this "with reasonable particularity," then the foregone conclusion doctrine applies, meaning that the information is not covered within the scope of the privilege and the compelled production of the information does not violate the Fifth Amendment guarantee against self-incrimination.[131]

C. Lower Courts' Interpretation of the Right Against Self-Incrimination Using Supreme Court Precedent

Despite a storied jurisprudence on the testimonial component of the right against self-incrimination,[132] the Supreme Court has yet to decide a self-incrimination case involving encrypted devices. However, several lower courts have applied Supreme Court precedent in encryption cases

126. *Id.*
127. *Id.*
128. An extensive discussion of the foregone conclusion doctrine is not necessary here because the factual scenario this Comment analyzes—namely, whether compelled production of fingerprints onto a smartphone device—does not implicate the doctrine since law enforcement officers execute the warrants without knowing of any specific incriminating information on these people's devices.
129. Fisher v. United States, 425 U.S. 391, 411 (1976).
130. United States v. Greenfield, 831 F.3d 106, 115–16 (2d Cir. 2016) (SUBS HISTORY).
131. *Fisher*, 425 U.S. at 411; *see Greenfield*, 831 F.3d at 116.
132. *See generally supra* Sections III.A. & III.B.

involving passwords on phones and computers.[133] Attention must be given to these cases to accurately assess whether courts would consider compulsion of fingerprints to access smartphone devices a violation of the privilege against self-incrimination.

In *In re Grand Jury Subpoena Tecum Dated March 25, 2011*, the Eleventh Circuit Court of Appeals held that compelling a defendant to give up his computer password so the government could decrypt files on his hard drive was a violation of the right against self-incrimination.[134] The court determined that requiring an individual to disclose his password to decrypt his files and make them accessible to the government is a testimonial act because the individual reveals "contents of [his] mind" in the process.[135]

In 2010, the U.S. District Court for the Eastern District of Michigan in *United States v. Kirschner* similarly addressed whether compelling a defendant to produce his computer password implicated the right against self-incrimination.[136] In *Kirschner*, the government subpoenaed an individual, compelling him to provide all passwords associated with his computer or with files on his computer,[137] to look for alleged evidence of child pornography located in the individual's encrypted computer files.[138] The defendant resisted the subpoena on the grounds that such compulsion violated his right against self-incrimination.[139] The court agreed with the defendant and held that the subpoena did, in fact, violate the constitutional rights of the defendant[140] because producing a computer password was analogous to producing a wall safe combination that resides in the mind of an individual.[141] In the court's view, providing a decryption password was "about producing specific testimony asserting a fact" and, thus, testimonial evidence that enjoyed protection under the privilege against self-incrimination.[142]

State courts also have looked at how self-incrimination jurisprudence applies to cases involving encrypted devices. The Supreme Judicial Court of the Commonwealth of Massachusetts analyzed article 12 of its state constitution—the equivalent of the federal Constitution's Fifth Amendment—to determine whether compelled production of a computer's en-

133. *See generally In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, United States v. John Doe, 670 F.3d 1335 (11th Cir. 2012) (Nos. 11-12268, 11-15421); United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010); Commonwealth v. Gelfgatt, 468 Mass. 512 (2014); Commonwealth v. Baust, 89 Va. Cir. 267 (2014).

134. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d at 1352–53.

135. *Id.* at 1341, 1346.

136. *Kirschner*, 823 F. Supp. 2d at 668.

137. *Id.* at 666.

138. *Id.* at 667.

139. *Id.* at 668.

140. *Id.*

141. *Id.* at 668–69 (stating that United States v. Hubbell, 530 U.S. 27, 43 (2000) resolved that something analogous to a wall safe that only resides in an individual's mind is testimonial.)

142. *Kirschner*, 823 F. Supp. 2d at 669.

cryption key violated the right against self-incrimination.[143] The self-incrimination analysis used by the Massachusetts courts, just like federal precedent, precludes protection under the privilege if the information sought is physical or non-testimonial evidence.[144] Under this court's view, a testimonial action is any action that reflects the "knowledge, understanding, and thoughts" of the accused.[145]

Applying this rationale, the court observed that, "at first blush," the defendant's governmentally-compelled act of decrypting his computer would appear testimonial because it would acknowledge the defendant's "ownership and control [over] the computer[ ]" and "be a communication of his knowledge about particular facts that would be relevant to the Commonwealth's case."[146] However, the court held that the evidence ultimately did not amount to testimonial evidence because "the factual statements that would be conveyed by the defendant's act of entering an encryption key . . . [were] 'foregone conclusions'" given that the government knew with reasonable particularity of the existence, control, and authenticity of the incriminating evidence.[147] In her dissent, Justice Lenk said that such an order should be deemed a violation of an individual's right against self-incrimination because it "is the functional equivalent of requiring him to produce the unencrypted contents of the devices seized."[148]

Pertinent to this Comment's focus, a Virginia trial court recently heard a case regarding the right against self-incrimination in the context of smartphones encrypted using fingerprint authentication.[149] The Virginia court held that, pursuant to the privilege against self-incrimination, a suspect "cannot be compelled [by the police] to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same."[150] The Virginia court determined that a fingerprint, unlike a passcode, is not an artifact of the defendant's mind that is kept entirely within the confines of his mind.[151] In the court's analysis, revealing a password invariably requires a person to divulge his mental processes and, thus, is protected testimonial evidence under the Fifth Amendment.[152] Conversely, "[t]he fingerprint like a key . . . does not require the witness to divulge anything through his mental processes" and, thus, cannot be characterized as testimonial evidence subject to the privilege against self-incrimination.[153] For the Virginia trial court, compelling an individual to produce a fingerprint to unlock a smartphone is analogous

143. Commonwealth v. Gelfgatt, 468 Mass. 512, 513–14 (2014).
144. *Id.* at 525.
145. *Id.* at 525–26.
146. *Id.* at 522.
147. *Id.* at 523–24.
148. *Id.* at 527–28 (Lenk J., dissenting).
149. Commonwealth v. Baust, 89 Va. Cir. 267 (2014).
150. *Id.* at 271.
151. *Id.*
152. *Id.*
153. *Id.*

to ordering a DNA sample or a key—it is constitutionally permissible because it involves compulsion of physical evidence and not testimonial evidence.[154]

More recently, in *State v. Diamond*, a Minnesota state appellate court faced this issue as a matter of first impression.[155] Like the Virginia court in *Baust*, the Minnesota court concluded that forcing a person to produce his fingerprint or thumbprint to unlock his smartphone does not implicate his right against self-incrimination.[156] In this fact pattern, an individual suspected of burglary and theft was compelled by court order, based on probable cause, to press his fingerprint or thumbprint on his smartphone so the police could search it.[157] After the individual initially refused to comply, asserting his privilege against self-incrimination, threat of civil contempt eventually led him to comply, and the search revealed incriminating evidence against him.[158] The individual submitted a motion to suppress the evidence found on his cellphone, which the district court denied.[159]

On appeal, the court held that the individual's Fifth Amendment privilege against self-incrimination was not violated because compelled production of a fingerprint is not testimonial.[160] In the court's view, the action was not testimonial because, unlike decrypting a hard drive or producing the combination to a safe, the individual "was not required to disclose any knowledge he might have or to speak his guilt."[161] For it to be protected testimonial activity, the activity must involve some "level of knowledge and mental capacity" and cannot be the compelled production of mere physical characteristics or attributes.[162] Additionally, the court asserted that the non-testimonial nature of pressing a fingerprint on a smartphone to unlock it is not overcome by the fact that such an action necessarily shows exclusive control over the smartphone and the information contained inside it.

154. *Id.*
155. 890 N.W.2d 143, 149 (Minn. Ct. App. 2017) (SUBS HISTORY).
156. *Id.* at 151.
157. *Id.* at 145–46.
158. *Id.* at 146, 150.
159. *Id.* at 146.
160. *Id.* at 151.
161. *Diamond*, 890 N.W.2d at 150.
162. *Id.* at 151.

IV. ANALYZING WHETHER COMPELLED FINGERPRINT PRODUCTION TO UNLOCK A SMARTPHONE DEVICE VIOLATES THE RIGHT AGAINST SELF-INCRIMINATION

A. Under Current Jurisprudence, Compelled Fingerprint Production to Unlock a Smartphone Does Not Violate the Right Against Self-Incrimination

Under current Supreme Court precedent, courts are likely to employ the same rationale as the lower courts in the Virginia and Minnesota cases[163] in determining if compelling fingerprints to unlock a phone violates a citizen's right against self-incrimination. Like the decisions of the lower courts discussed *supra*,[164] courts are likely to view an individual's production of a fingerprint to unlock a smartphone merely as a source of "real or physical evidence"[165] and not testimonial in nature because it does not communicate "contents of [the] mind."[166] Therefore, courts likely will reach the conclusion that compelled production of a fingerprint to unlock a phone is a non-testimonial act and, thus, not protected under the right against self-incrimination.

The operative legal framework dictates that fingerprints, regardless of their actual function, generally will be viewed as real or physical evidence, meaning that the government has the right to freely compel their production without violating the right against self-incrimination.[167] As the lower courts correctly point out, a password is qualitatively different than tangible, bodily evidence.[168] A password's exact sequence, typically in some form of alpha-numerical sequence, resides in the depths of our minds. Thus, it follows that when the government compels an individual to produce his password in an investigation, the individual is being asked to make use of his mental faculties[169] and "to disclose any knowledge he might have,"[170] namely the characters and order of those characters that make up his password. Communicating a password to a law enforcement officer "explicitly . . . relate[s] a factual assertion"[171] that is fundamentally a testimonial, communicative act.[172]

A fingerprint, on the other hand, has none of these qualities. A fingerprint is tangible, bodily evidence that is not located within an individual's

163. *See generally id.*; Commonwealth v. Baust, 89 Va. Cir. 267 (2014).
164. *See supra* Section III.C.
165. *See* Schmerber v. California, 384 U.S. 757, 764 (1966).
166. United States v. Hubbell, 530 U.S. 27, 43 (2000).
167. *See* Soares, *supra* note 91, at 2004–05.
168. *See In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1341, 1346 (11th Cir. 2012); United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010); Commonwealth v. Gelfgatt, 468 Mass. 512, 525–26 (2014); *Baust*, 89 Va. Cir. at 271.
169. *See Hubbell*, 530 U.S. at 43.
170. *See* United States v. Wade, 388 U.S. 218, 222 (1967).
171. *See* Doe v. United States, 487 U.S. 201, 210 (1988).
172. *See* Holt v. United States, 218 U.S. 245, 252–53 (1910).

mind.[173] It is an identifying physical characteristic,[174] much like someone's voice[175] or handwriting.[176] Hence, providing a fingerprint to unlock a smartphone is more akin to providing a "key to a strongbox" than "the combination to a wall safe" because it involves surrendering something with a physical substance, as opposed to a mental configuration, to access possibly incriminating information.[177] Under the current state of the law, when the government compels an individual to press his fingerprint on his phone to unlock it, the government compels "the accused to exhibit his *physical characteristics*, not . . . to disclose any knowledge he might have."[178]

In the factual scenario at hand,[179] although the government would be compelling an individual to unwillingly participate in the collection of evidence potentially used to incriminate him by forcing him to press his fingerprint on his smartphone to unlock it,[180] the very act itself of producing a fingerprint, like a blood sample, likely would be considered non-testimonial.[181] Therefore, because governmentally-compelled production of a fingerprint is non-testimonial, the Central District of California correctly concluded in its memo that the right against self-incrimination likely is not implicated.[182] As *TIME* magazine astutely observed, despite cell phone manufacturers proudly touting that features like fingerprint authentication enhance the security of devices,[183] the reality is that "data protected only by an old-school passcode is afforded stronger legal protection under the Fifth Amendment."[184]

B. A Call to Return the Principle of Privacy to Self-Incrimination Jurisprudence

It has been previously acknowledged that "[t]echnology has outgrown the Supreme Court's Fifth Amendment jurisprudence."[185] Although current self-incrimination precedent leads to the conclusion that compelled fingerprint production to unlock a phone does not implicate the right against self-incrimination,[186] the outcome should be different. In deciding what is protected testimonial evidence, it is imperative for courts to shift

173. *See Hubbell*, 530 U.S. at 43.
174. *See Wade*, 388 U.S. at 222–23.
175. *See* United States v. Dionisio, 410 U.S. 1, 7 (1973).
176. *See* Gilbert v. California, 388 U.S. 263, 266–67 (1967).
177. *See Hubbell*, 530 U.S. at 43.
178. *See Wade*, 388 U.S. at 222 (emphasis added).
179. *See supra*, Section I.A.
180. *See* Schmerber v. California, 384 U.S. 757, 761 (1966).
181. *See id.* at 765.
182. *See* Memorandum, *supra* note 4, at 3.
183. *See Touch ID, supra note 21.*
184. Jack Linshi, *Why the Constitution Can Protect Passwords but Not Fingerprint Scans*, Time (Nov. 6, 2014), http://time.com/3558936/fingerprint-password-fifth-amendment/ [https://perma.cc/SFR7-Q649].
185. Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. Pa. J. Const. L. Heightened Scrutiny 11, 11 (2012).
186. *See generally supra* Section IV.A.

away from the physical versus communicative dichotomy[187] if the privilege against self-incrimination is to be protected from being "eviscerated by emerging technologies."[188] The need to shift away from this long-used distinction is borne out of the rapidly changing technological landscape in which we live. For example, Susan Brenner, a law professor at the University of Dayton, views the current approach to testimonial evidence as outdated for our current environment.[189] "It isn't about fingerprints and the biometric readers," Brenner stated, but rather about "the contents of [a] phone, much of which will be about [people], and . . . that could be incriminating."[190]

Brenner perceptively notes that in our ever-changing technological world—where fingerprints, retinas, and other sources of biometric data are proliferating encryption sources in mobile devices[191]— courts should cautiously exercise their judicial capacities so as to not violate the intrinsically valuable right to privacy enshrined in the Constitution by giving the government unimpeded access to the private contents in people's smartphones.[192] In relying on the physical versus communicative distinction, courts have imperiled a principle of "great probative force" that has served as a compelling justification for the privilege against self-incrimination: the principle of individual privacy.[193]

Even though compelling someone to provide a fingerprint to unlock a phone is functionally equivalent to forcing that same person to provide an alpha-numerical password for that same phone, courts have chosen to treat these two methods of encryption differently because of the judiciary's steadfast reliance on the outdated distinction between physical and communicative evidence.[194] There is no meaningful difference between fingerprints and passwords in the context of encrypted smartphones and the right against self-incrimination; both methods of encryption function to make private information inaccessible to third parties. Therefore, in deciding the scope of the privilege, it is improper to treat compelled fingerprint production to unlock a smartphone the same as compelled physical or real evidence because mere physical evidence, like a blood sample, "is readily separable from what we think important about us, whereas

187. *See* Holt v. United States, 218 U.S. 245, 252–53 (1910).

188. Mohan & Villasenor, *supra* note 186, at 11.

189. Ben Lovejoy, *FBI Granted Federal Court Warrant Forcing Suspect to Unlock iPhone Using Touch ID*, 9TO5MAC (May 2, 2016, 4:06 AM), https://9to5mac.com/2016/05/02/federal-court-touch-id-fingerprint/ [https://perma.cc/MR6F-R3C4].

190. *Id.*

191. *See Biometrics Report*, *supra* note 78; Whitney, *supra* note 79; *see also* Michael Corkery, *Goodbye, Password. Banks Opt to Scan Fingers and Faces Instead*, N.Y. TIMES (June 21, 2016), https://www.nytimes.com/2016/06/22/business/dealbook/goodbye-password-banks-opt-to-scan-fingers-and-faces-instead.html [https://perma.cc/C7HU-TTS3] (noting that banks are moving toward facial and fingerprint scans for enhanced security).

192. *See supra* Section III.A.

193. McKay, *supra* note 88, at 213–14; *see* Note, *Formalism, Legal Realism, and Constitutionally Protected Privacy Under the Fourth and Fifth Amendments*, 90 HARV. L. REV. 945, 951 (1977).

194. *See, e.g.*, Holt v. United States, 218 U.S. 245, 252–53 (1910).

[the contents of our phones like our] thoughts are not."[195]

Fingerprint authentication "acts like a password. [It is] a simple password, but [it is] still a password."[196] At a rudimentary level, compelling an individual to decrypt his smartphone, whether by compelling production of a fingerprint or a password, gives the government unbounded access to information, much of which is private in nature and potentially incriminating. Commenting on the legality of compulsion of fingerprints to unlock a smartphone, criminal defense attorney Hayes Hunt remarked that "once we put a password on something or on ourselves, we have a certain privacy interest."[197] For the courts to suggest that fingerprints are dissimilar to passwords amounts to nothing more than a "clever end-run" around a citizen's right to be free from incriminating himself with his own private information.[198]

Thus, courts should actively look to reincorporate the principle of privacy to the nucleus of self-incrimination analysis when deciding if an action is testimonial or not. Doing so will ensure that the courts are adapting to the unexpected changes that accompany technological development. More importantly, it would protect individuals from arbitrary legal distinctions that beget different outcomes in functionally similar situations, such as allowing the government to access private information on a person's smartphone if they use fingerprint authentication but not if they use an alpha-numerical password. To determine how the principle of privacy should be reincorporated, it is necessary to review the role the principle has played in the past with respect to this right.

1. Supreme Court's Views on the Principle of Privacy and the Right Against Self-Incrimination

Justice Felix Frankfurter wisely remarked that in interpreting the Fifth Amendment "a page of history is worth a volume of logic."[199] Retrospectively looking at how the Supreme Court has viewed rights under the Fifth Amendment, it is discernable that the principle of privacy once served as a fundamental justification for the right against self-incrimination.[200] In fact, scholars have recognized that "the claim that compelled self-incrimination is an improper and impermissible invasion of a person's right to privacy" is "[o]ne of the most popular justifications for the privilege against self-incrimination."[201] The Supreme Court has, on various

195. Dov Fox, Article, *The Right to Silence as Protecting Mental Control*, 42 AKRON L. REV. 763, 796 (2009).

196. Orin Kerr, *The Fifth Amendment and Touch ID*, WASH. POST (Oct. 21, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/21/the-fifth-amendment-and-touch-id/?tid=a_inl&utm_term=.4654e54a3b27 [https://perma.cc/ZU9K-RCEC].

197. Linshi, *supra* note 185.

198. *See* Turner, *supra* note 23.

199. Ullman v. United States, 350 U.S. 422, 438 (1956) (quoting N.Y. Trust Co. v. Eisner, 256 U.S. 345, 349 (1921)).

200. David Dolinko, *Is There A Rationale for the Privilege Against Self-Incrimination?*, 33 UCLA L. REV. 1063, 1090, 1107 (1986).

201. Tarallo, *supra* note 92, at 168–69 (citing Dolinko, *supra* note 201, at 1107).

occasions, endorsed this justification for the privilege against self-incrimination.[202] For example, as early as 1928, Justice Brandeis, writing in dissent, noted that the Fifth Amendment is one of the primary constitutional pillars of the right to privacy because it protects citizens from governmental "invasion[ ] . . . of the sanctities of a man's home and the privacies of life."[203]

Furthermore, in *Murphy v. Waterfront Commission of New York Harbor*, Justice Goldberg expressed that privacy is one of the "fundamental values and most noble aspirations" the country's founders sought to protect in the Fifth Amendment.[204] In Justice Goldberg's view, freedom from self-incrimination is not only a valuable shelter for the guilty against abusive government techniques, but also a valuable shield for the innocent from having the government violate their "human personality" by disrespecting their "private enclave" and "private life."[205]

Moreover, in his majority opinion in *Griswold v. Connecticut*, Justice Douglas noted that "[v]arious guarantees create zones of privacy. . . . The Fifth Amendment in its [s]elf-[i]ncrimination [c]lause *enables the citizen to create a zone of privacy* which government may not force him to surrender to his detriment."[206] Justice Goldberg's and Justice Douglas's articulations of the inviolable principle of privacy, thus, reflect the profound Western tradition for respecting the intrinsic value of personal privacy that "inheres" by virtue of being human.[207] Thus, the right against self-incrimination derives justification from the notion that an individual's privacy is violated when others obtain his sensitive personal information contrary to his wishes.[208]

Evidently, the privilege against self-incrimination has historically functioned in large part "to protect a 'natural individual from compulsory incrimination through his own testimony or personal records.'"[209] Compelling a suspect to involuntarily give the government access to a device containing his greatest intimacies undermines the value the Fifth Amendment and other constitutional provisions place on individual privacy. After all, smartphone devices represent "the microcosm of an individual"[210] on account of how society uses them. Hence, courts should shy away from using feeble distinctions between communicative and physical evidence in determining which activities are testimonial and which are

---

202. *Id.* at 168.

203. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (quoting Boyd v. United States, 116 U. S. 616, 630 (1886)).

204. 378 U.S. 52, 55 (1964).

205. *Id.* (quoting United States v. Grunewald, 233 F.2d 556, 581–82 (2d Cir. 1956) (Frank, J., dissenting), *rev'd*, 353 U.S. 391 (1957)).

206. 381 U.S. 479, 484 (1965) (emphasis added).

207. *Formalism, Legal Realism, and Constitutionally Protected Privacy Under the Fourth and Fifth Amendments*, *supra* note 194, at 986.

208. *See* Dolinko, *supra* note 201, at 1108.

209. Andresen v. Maryland, 427 U.S. 463, 470–71 (1976) (quoting Bellis v. United States, 417 U.S. 85, 89 –90 (1974)).

210. Whitten, *supra* note 58, at 1–2.

not to avoid coercing individuals from revealing the private contents found in their smartphones.[211] Instead, courts should limit the government's access to what is, together with the human mind, "the 'most private preserve of our ordinary lives'": our smartphone devices.[212]

Although the Fifth Amendment does not, by its language, guarantee a general right of privacy, the Supreme Court has opined that the individual right "to a private enclave" and "a private life" is central to the spirit of the right against self-incrimination.[213] When the legal system allows the government to indiscriminately access the smartphones of its citizens by virtue of an outdated distinction, in effect it permits the government to unimpededly look through what has been properly described "as [an] extension[ ] of ourselves."[214] This amounts to governmental intrusion upon the "most private preserve of our ordinary lives, the place inside everyone's head where secrets reside."[215]

2. Philosophical Considerations

Renowned legal scholar David Dolinko has argued against a privacy-based rationale to support the right against self-incrimination.[216] Dolinko argues that if the purpose of the privilege is to protect individual privacy, "why should it rule out only one special type of infringement of privacy," namely government-compelled self-incrimination?[217] In his view, an individual's privacy is always infringed, some way or another, whenever potentially incriminating information about a person is revealed against his wishes.[218] Dolinko sees no qualitative difference between the government compelling an individual to disclose information about himself and the government acquiring that same incriminating evidence by independent means.[219] Therefore, Dolinko posits that because individual privacy is always violated when a person's information is obtained contrary to his or her wishes—regardless of how it is obtained—then the principle of privacy cannot serve as a legitimate justification for the right against self-incrimination.[220]

However, Dolinko fails to recognize that these situations are significantly and qualitatively different from a privacy standpoint, particularly in the context of smartphones. Notably, when the government compels an

---

211. *See* Holt v. United States, 218 U.S. 245, 252–53 (1910).

212. Barillare, *supra* note 93, at 997 (quoting Robin Marantz Henig, *Looking for the Lie*, N.Y. TIMES, Feb. 5, 2006, § 6 (Magazine), at 47, 50 [DISCUSSING the quote and its original reference])

213. Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55. (quoting United States v. Grunewald, 233 F.2d 556, 581 –82 (2d Cir. 1956) (Frank, J., dissenting), *rev'd*, 353 U.S. 391 (1957)).

214. *See* Lynch, *supra* note 45.

215. Barillare, *supra* note 93, at 997 (quoting Robin Marantz Henig, *Looking for the Lie*, N.Y. TIMES, Feb. 5, 2006, § 6 (Magazine), at 48).

216. *See* Dolinko, *supra* note 201.

217. *Id.* at 1109.

218. *See id*. at 1109–15.

219. *See id.*

220. *See id.* at 1136–37.

individual to reveal information about himself instead of obtaining that same information through secondary or other objective sources, the individual risks disclosing additional information that he sought to keep private and unbeknownst to the world. Each person keeps private certain information in the precipices of his mind—or nowadays his mobile device—that is intended to be accessible only by himself.

When the government compels an individual to reveal the contents of his mind, or in this case, the contents of his smartphone by providing a fingerprint, the individual risks disclosing private information that he intends to keep away from the rest of the world. However, if the government accesses the contents of a person's cellphone by means other than compulsion, then that information would not be considered private *per se*, as there would be a public or secondary means of accessing it. This necessarily means that the individual, either explicitly or implicitly, made that information public at some prior point in time, inherently making it lose any private qualities it had. Therefore, what Dolinko overlooks is the value of an individual's capacity to "modulate the amount" and character of information that he makes "known to others."[221] After all, "privacy . . . is the *control* we have over information about ourselves."[222] When the government compels an individual to give it unrestricted access to his smartphone, it strips that individual of what should be his ability to have complete control over the information he has decided to keep private.[223]

Considering the importance of this principle of privacy, the government should avoid forcing individuals to surrender control of the modulation capacity they have over their own personal information. Instead, the government should preserve this capacity by fashioning new standards in the self-incrimination context that are sensitive to the private nature of personal devices like smartphones. A first step would be for courts to reevaluate the value behind the physical versus testimonial dichotomy and analyze its consequences when applied to smartphones and other types of technological devices. Second, courts must reincorporate the principle of privacy to their self-incrimination analyses to avoid infringing on citizens' rightful control over the private information they wish to keep secret within their devices. Courts can accomplish this by reinvigorating the principle of privacy as a basic justification for the right against self-incrimination, and consequently, preventing the government from compelling individuals to give it unrestricted access to their most personal information against their will.

221. Robert S. Gerstein, *Privacy and Self-Incrimination,* 80 ETHICS 87, 89 (1970) (citing Charles Fried, *Privacy*, 77 YALE L. J. 475, 478–85 (1968)).

222. *Id.* (quoting Fried, *supra* note 223, at 482).

223. *Id.* at 90.

C. Additional Issues to Be Explored—Fourth Amendment Particularity

The issuance of these warrants also raises serious Fourth Amendment questions.[224] Interestingly, one glaring omission from the government's memorandum is any discussion on whether the warrant met the Fourth Amendment's particularity requirement.[225] The Supreme Court has made clear that, generally, the government must obtain a warrant before searching an individual's cell phone for information.[226] However, the Fourth Amendment also mandates that warrants be particular in describing the places and persons to be searched and seized.[227] The framers imposed the particularity requirement to avoid the issuance of general warrants that sanction searches which encroach on an individual's privacy.[228] Justice Brennan noted that the general warrant is "often regarded as the single immediate cause of the American Revolution."[229]

Legal experts have raised serious concerns over the particularity of the warrant issued in the Los Angeles case,[230] which gives law enforcement officers broad authority to search "*any person* who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device."[231] Jennifer Lynch, a senior staff attorney at the Electronic Frontier Foundation, cited her concerns about the government's warrant being "so broad in scope" and for relying on "outdated cases" to give it access to a "vast amount of data that's on [smartphones]."[232]

Phones contain the private lives of individuals, including their personal conversations, list of friends and family members, and intimate pictures of themselves and others. If courts provide law enforcement unimpeded access to these devices based purely on speculation and the hope of finding something of incriminating value with no regard for specifics, it permits an invasive and unjustified intrusion into the private life of an individual contained in that pocket-sized device. Lynch worries that "[i]f this kind of thing became law then there would be nothing to prevent . . . a search of every phone at a certain location."[233]

Several solutions to remedy these intrusive searches into mobile devices have been proposed. A good first step was for the Supreme Court in

---

224. *See* Kerr, *supra* note 2.
225. *See* Memorandum, *supra* note 4, at 5–7.
226. Riley v. California, 134 S. Ct. 2473, 2485 (2014).
227. *See* U.S. Const., amend. 4 ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, *and particularly describing the place to be searched, and the persons or things to be seized.*" (emphasis added)); *see* Ybarra v. Illinois, 444 U.S. 85, 91 (1979).
228. Collins T. Fitzpatrick, *Protecting the Fourth Amendment So We Do Not Sacrifice Freedom for Security*, 2015 Wis. L. Rev. 1, 4–5 (2015).
229. Lopez v. United States, 373 U.S. 427, 454 (1963).
230. *See* Fox-Brewster, *supra* note 3; Kerr, *supra* note 2.
231. Memorandum, *supra* note 4, at 1–2 (emphasis added).
232. *See* Fox-Brewster, *supra* note 3.
233. *Id.*

Riley to unequivocally demand that law enforcement officials obtain warrants before rummaging through the contents of an individual's cell phone.[234] However, a further step in the right direction would require legislators to enact laws that mandate that warrants be highly specific, describing in detail the information expected to be found in a phone, as opposed to merely claiming that the phone may contain evidence of a crime.[235] In any event, ample room for discussion remains on this particular topic, which legal scholars should explore in greater depth.

V. CONCLUSION

We have entered a new world, but as the Supreme Court recognized in *Riley*,[236] our old values should still apply and be invoked to limit the government's ability to dig through the intimate details of our private lives, which day by day are increasingly found in our personal mobile devices. As our adoption of evolving personal digital technologies continues, courts and legislators at both the federal and state levels must take corresponding steps forward into the digital age to ensure our fundamental rights and guaranteed freedoms are neither curtailed nor eroded.

In light of the contemporary societal departure from passwords to biometric data as a form of decryption,[237] it is imperative that courts extend the standard they have set for passwords as testimonial activity to encompass biometric tools that function the same as passwords. Just as sensibilities toward the principle of privacy have led the Court in the past "to block legislative attempts to control intimate private conduct"—abortion, right to martial privacy, private possession of obscene material—governmental intrusion into the individual's private life should be prohibited under the Fifth Amendment "rather than tolerated as a necessary incident of criminal law enforcement."[238] Merely believing that someone may be involved in criminal conduct should not outweigh the interests of privacy the Constitution holds dear.[239]

It is inevitable that "[t]he right against self-incrimination has bedeviled the Court with hard value choices."[240] The right against self-incrimination will continue to bedevil our courts in this digital era until they make a deliberate value choice to adapt their understanding of this right to comport with new technological advances in a way that is faithful to the guarantees of privacy the framers sought to protect in the Constitution.

234. Riley v. California, 134 S. Ct. 2473, 2495 (2014).
235. Whitten, *supra* note 58, at 1, 30.
236. *Riley*, 134 S. Ct. at 2495.
237. *See* Corkery, *supra* note 192.
238. *Formalism, Legal Realism, and Constitutionally Protected Privacy Under the Fourth and Fifth Amendments*, *supra* note 194, at 986.
239. *Id.*
240. Alfredo Garcia, *The Fifth Amendment: A Comprehensive and Historical Approach*, 29 U. TOL. L. REV. 209, 211 (1998).